REMARKS

I. Introduction

Claims 1-20 are pending in the application.

Claims 1-3, 8-11, 13, 16 and 19 are currently amended. Claims 4-7, 12, 14, 15, 17, 18 and 20 are as originally filed.

Claims 1-7 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Willins et al. U.S. Patent Publication No. 2002/0152391 A1 in view of Novikov et al. et al. U.S. Patent 6,282.304, Chang et al. et al. U.S. Patent Publication No. 2002/0122415, Patel U.S. Patent Publication No. 2002/0174345 and Moquin U.S. Patent Publication No. 2002/0106077 A1.

Claim 8 was rejected under 35 U.S.C. §103(a) as being unpatentable over Willins et al., Novikov et al., Chang et al., Moquin, and Miller U.S. Patent Publication No. 2003/0046557.

Claim 9 was rejected under 35 U.S.C. § 103(a) as being unpatentable over Novikov et al., Chang et al., Moquin and Patel.

Claims 10-12 were rejected under 35 U.S.C. § 103(a) as unpatentable over Novikov et al., Chang et al., Moquin, and Patel and further in view of the examiner's official notice.

Claims 13 and 16 were rejected under 35 U.S.C. § 102(b) as being anticipated by Srey et al. U.S. Patent 6,141,436.

Claims 14 and 17 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Srey et al. and Holt U.S. Patent 6,404,862.

Claims 15 and 18-20 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Srey et al. and the examiner's official notice.

Reconsideration of this application in light of the following remarks is respectfully requested.

II. Rejections Based on 35 U.S.C. § 102(b) (Paragraph 2 of Office Action)

Claims 13 and 16 were rejected under 35 U.S.C. § 102(b) as anticipated by Srey et al. Applicants respectfully traverse this rejection as it may be applied to amended claims 13 and 16.

In claims 13 and 16, as amended, the finger image sensor is positioned on the second major side of the handset (or handset portion in claim 16), and the contoured surface is at least partially positioned on the second major side of the handset (or the first portion thereof) extending from the second end of the handset (or first portion thereof) leading to the finger-image sensor. Claims 13 and 16, as amended, recite that the contoured surface is configured to guide a distal portion of a human finger onto the finger image sensor longitudinally with respect to the finger and to receive a portion of the finger longitudinally adjacent to the distal portion when the distal portion is positioned on the finger image sensor.

The telephone shown in Fig. 5 of Srey et al., for example, does not include a contoured surface leading to a finger image sensor. Fig. 5 of Srey et al. shows a scanner 115 positioned on a flat surface with no contoured surface leading to the scanner. In the embodiment depicted in Fig. 4 of Srey et al., the scanner 115 is positioned on the side of the telephone (not a major side), and there does not appear to be any contoured surface leading to the scanner. To the extent that one considers that

the telephone shown in Fig. 3 of Srey et al. includes a contoured surface adjacent the scanner 115 on the side of the telephone, applicants submit that any such surface does not lead to the scanner and is not configured to guide a distal portion of a human finger onto the scanner 115 longitudinally with respect to the finger and to receive a portion of the finger longitudinally adjacent to the distal portion when the distal portion is positioned on the scanner, as claimed in claims 13 and 16. Moreover, applicants point out that in the telephone depicted in Fig. 3 of Spry, the scanner 115 is not positioned on a major side of the telephone, as claimed in claims 13 and 16.

For the reasons given above, applicants submit that claims 13 and 16, as amended, are not anticipated by, and are allowable over, Srey et al.

III. Rejections Based on 35 U.S.C. § 103(a) (Paragraphs 4-9 of Office Action)

Claims 1-12, 14-15, and 17-20 were rejected under 35 U.S.C. § 103(a), as being unpatentable in view of various combinations of the references cited above.

Claims 1-8 (Paragraphs 4 & 5 of Office Action)

The examiner rejected claim 1 as being unpatentable over Willins et al. combined with Novikov et al., Chang et al., Moquin and Patel. Applicants traverse this rejection as it may be applied to amended claim 1.

Claim 1 claims a system for enabling use of a computer terminal in a network to access or otherwise participate in at least one network-related function and voice communication over the network. The claimed system comprises a telephone handset including a microphone and a speaker coupled to provide signals to and receive signals from the computer terminal for voice communication, and a finger image sensor coupled to at least to provide signals to the computer terminal relating to a finger-image

sensed by the finger-image sensor. The system also includes means responsive to the authenticating means for enabling the computer terminal in the network to access or otherwise participate in the performance of at least one network-related function and voice communication over the network at least from each computer terminal for which a sensed finger-image was authenticated.

Thus, responsive to the authenticating means, means enable the computer terminal in the network to access or otherwise participate in the performance of at least one network-related function and voice communication over the network at least from each computer terminal for which a sensed finger-image was authenticated. A system including at least such means is not described in the prior art of record.

We show below that none of the five references applied by the examiner in the rejection of claim 1 describes such means individually or in combination.

The examiner contends (Office Action, page 4, lines 1-3 and 6-10) that Willins et al. discloses a system enabling the use of a computer terminal in a network to access or otherwise participate in at least one network-related function and voice communication which comprises means responsive to the authenticating means for enabling the computer terminal to access or otherwise participate in the performance of at least one network-related function and voice communication over the network at least from each computer terminal providing finger-image-related signals based upon which a sensed finger image was authenticated. The examiner references paragraphs 61-64 and 66-69 of Willins et al.

Willins et al. discloses that biometric data be used to perform encryption or decryption on input data and for verification for purposes of access to a network. See, e.g., paragraphs 48, 65, 69 (decryption of input data), paragraphs 62, 63, 69

(verification by end or remote server. or system), paragraphs 51, 64 (verification by client followed by verification by remote server).

Willins et al. does not disclose that such verification provide access to both at least one network-related function and voice communication. Instead, Willins et al. extensively discusses access to wireless LAN networks, and mentions that "in the context of an IP network using VOIP," an access point may also serve as an H.323 Gatekeeper or Gateway. Willins et al.'s mention of "VOIP" in paragraph 66 is quoted below in context with surrounding language:

> **[0066]** FIG. 3 is a block diagram of a secure network architecture using the present invention. The mobile computer 300 is illustrated as being in communication with an access point 302. The association and roaming properties of a mobile computer in an IEEE 802.11 wireless network have been described above, and need not be repeated here. In the context of an IP network using VoIP, which is one of the areas of application of the present invention, the access point 302 may also serve as an H.323 Gatekeeper or Gateway. The mobile computer 300 may roam from access point to access point in the WLAN, and even from one ESS to another ESS. Although WEP may be used, at the radio frequency MAC level, enhanced security requires software protocols above the MAC level. The use of a user biometric 301 is a key feature according to the present invention for providing this enhanced security.

As shown in Fig. 3 of Willins et al., to which paragraph 66 refers, mobile computer 300 accesses the network 303 through an access point 302, which may be an H.323 Gatekeeper or Gateway. (H.323 is a standard that supports voice, video, data, application sharing and whiteboarding.) As described in paragraph 69 of Willins et al., a source client 307 may provide data to mobile computer 300 via network 306, routers 305, network 303 and access point 302. Willens et al. only states that in the context of an IP network using VOIP, access point 302 may ***also*** serve as an H.323 Gatekeeper or Gateway. There is no disclosure that source clients 307 or mobile computers 300 can engage in voice communications and network related functions, but

only that mobile computer 300 can access the network 303 through an access point 302, which also serves as an H.323 Gatekeeper or Gateway. There is also no disclosure that if mobile computer 300 engages in voice communications, that it do so only after authentication.

Paragraphs 66 and 69 do not disclose enablement of voice communication responsive to authenticating means. In fact, except for mentioning "VOIP" in paragraph 66, Willins et al. does not address voice communication between mobile computers or between source devices or between mobile computers and source devices.

Fig. 1 of Willins et al., which depicts the architecture of a mobile computer (paragraph 52), does not include anything for carrying out voice communications. As pointed out above, although Willens et al. states that in the context of an IP network, using VoIP, the access point 302 may also serve as an H.323 Gatekeeper or Gateway, that statement does not disclose that the mobile computer 300 be enabled to engage in at least one network-related function ***and*** voice communication. There is also no disclosure in Willins et al. that biometric authentication is required in order to engage in voice communication by mobile computer 300.

It is submitted that if mobile computer 300 in Willins et al. can engage in voice communications over a network, that does not mean that authentication is required before mobile computer 300 can engage in voice communications with another mobile computer 300 or a source device 307 ***and also*** engage in network related functions. Willins et al. provides no disclosure whatsoever on this issue. As such, it is further submitted that the examiner should not otherwise read that functionality into Willins et al. without some basis to do so from Willins et al.

Novikov et al. discloses a mouse with a biometric input device for scanning a finger tip. Novikov et al. does not disclose voice communication capability. Like Willins et al., Novikov et al. does not disclose that authentication using the biometric input device on the mouse provides access to both at least one network-related function and voice communication.

Patel describes a transaction-based system that may use a telephone having a biometric input device (e.g., 28 in Fig. 6 of Patel). However, Patel does not disclose verification using the biometric input device on the telephone (or elsewhere in the Patel disclosure) to provide access to both at least one network-related function and voice communication.

Chang et al. relates to an Internet phone, and Moquin et al. relates to improvements in speakerphones. Neither is concerned with authentication.

Considering each of the five references discussed above individually, there is no disclosure in any reference of means responsive to an authenticating means for enabling the computer terminal in the network to access or otherwise participate in the performance of at least one network-related function ***and*** voice communication over the network at least from each computer terminal for which a sensed finger-image was authenticated.

The Examiner has failed to provide any reason for modifying Willins et al. and has failed to point to some teaching or suggestion within each of the references supporting any such modification.

In addition, in the system claimed in claim 1, a computer terminal in a network is enabled to access or otherwise participate in ***both*** at least one network related function and voice communication ***over the network*** responsive to an authenticating means.

An example of such a network is illustrated in Fig. 8 of the application. Novikov et al., Patel, Chang et al., and Moquin et al. disclose no such network. As such it would not be obvious to combine isolated features from any of these references with Willins et al. These references do not suggest that authentication enable both at least one network-related function and voice communication over the network for a terminal for which a sensed finger image was authenticated.

Applicants respectfully request that the obviousness rejection of claim 1 be withdrawn for the reasons discussed above.

In claim 2, as amended, the enabling means enables voice communication to and from only each terminal that provided finger-image-related signals based upon which a sensed finger-image was authenticated. This is not disclosed in Willins et al. or any of the other references discussed above.

It is submitted that amended claim 3 is allowable for reasons similar to those advanced for the allowance of claim 1.

Claims 4-8 are dependent upon claim 1 or claim 3. It is submitted these claims are allowable at least for the reasons advanced for the allowance of claim 1.

Claims 9-12 (Paragraphs 6-7 of Office Action)

Claim 9, as amended, claims apparatus for voice communication over a network through a computer terminal and for biometric identification, comprising a telephone handset including a microphone, a speaker, a finger-image sensor, circuitry coupled to the microphone and speaker which at least converts between analog and digital signals, and an interface coupling the finger-image sensor and the circuitry with the computer terminal. The claimed apparatus also comprises means associated with at least one of the computer terminal and the network for electronically authenticating a

finger-image sensed by the finger-image sensor based on the finger-image-related signals provided to that computer terminal, and means associated with at least one of the computer terminal and the network responsive to the authenticating means for enabling the computer terminal in the network to participate in voice communication over the network at least from each computer terminal for which a sensed finger-image was authenticated.

Claim 9 was rejected as being unpatentable over Chang et al, Novikov et al, Patel and Moquin et al. None of those references discloses apparatus including a telephone handset having a finger-image sensor, an interface coupling the finger-image sensor to a computer terminal, and means by which the computer terminal is enabled to participate in voice communication over the network.

None of the references is concerned with authentication for the purpose enabling a computer terminal to engage in voice communications. Chang et al. is not concerned with authentication. Novikov et al. discloses a mouse with a biometric input device, but does not disclose that the biometric input device be used to provide authentication in order to enable a computer terminal to engage in voice communications. The biometric device 28 in Patel is not used to enable a computer terminal to engage in voice communications, but to enable some kind of transaction (see paragraph 2 of Patel, for example). Mocquin et al. of course has nothing to do with authentication.

It is submitted that there is no disclosure in any of the four references applied by the examiner in the rejection of claim 11 that suggests the subject matter now claimed in amended claim 11. Therefore, withdrawal of the rejection of claim 11, and of claims 12-13 which are dependent upon claim 11, is requested.

Claims 14-15 and 17-18 (Paragraphs 8 and 9 of Office Action

Claims 14 and 17 are rejected over Srey et al. in combination with Holt (Office Action, pages 12-13). Applicants respectfully traverse these rejections.

Claims 14 and 17 are directed towards telephone handsets having opposed major sides with microphones and speakers positioned at opposite ends of the handset for conducting voice communication. The handset also includes a finger-image sensor for acquiring a fingerprint user to confirm user identification. The claims further specify that the handset does not include a keypad and therefore applicants' claimed invention cannot be used to enter numeric information such as a telephone number.

The examiner's proposed combination of the cellular phone described by Srey et al. and the modem-based authentication device of Holt, however, fails to produce such a device. Srey et al. discloses a conventional cellular telephone that includes a fingerprint identification system to improve telephone security. Srey et al. explains that the fingerprint identification system prevents unauthorized users from using the keypad on the telephone to place unauthorized calls (Srey et al., column 1, lines 22-50). The cellular telephone disclosed by Srey et al. obviously requires a keypad in order to perform its most basic function (*i.e.*, allowing the user to dial calls). Thus, removing the keypad would prevent the cell phone of Srey et al. from performing its primary function, strongly discouraging such a modification.

The purpose of the modem-based authentication device described by Holt is to provide an inexpensive electronic authentication means that does not have most of the features found on a conventional cell phone such as a display, keyboard, and microprocessor (Holt, column 1, lines 14-54). Holt explains that the authentication device operates in conjunction with a conventional telephone to provide a tone-based

response to a challenge signal via a smartcard to allow the owner of the authentication device system access (Holt, column 2, lines 37-64). The primary purpose of this system is to provide an inexpensive alternative to a full-function cellular phone that uses a smartcard. Thus, any attempt to modify this authentication device by adding traditional cellular phone features is expressly discouraged by the teaching of Holt.

Accordingly, because the teachings of Srey et al. strongly discourage the removal of the keypad from the disclosed cellular phone and because Holt expressly teaches away from the addition of traditional cell phone features to its authentication device, these references cannot be combined to produce applicants' invention claimed in claims 14 and 17. Moreover, even if these devices where combined as proposed by the examiner, the result would be a conventional cell phone with an authentication modem integrated into it, on which claims 14 and 17 clearly do not read.

In addition, it is submitted that claims 14-15, dependent upon claim 13, and claims 17-18, dependent upon claim 16, are allowable for the reasons advanced for claims 13 and 16, respectively.

Claims 19-20 (Paragraph 9 of Office Action)

Claims 19 and 20 were rejected over Srey et al. in combination with an official notice taken by the examiner. Applicants respectfully traverse.

In rejecting these claims, the examiner explained that brackets were well known in the art at the time of the invention, and that combining the prior art brackets with the cell phone of Srey et al. would produce a handset that can be hung to save workspace (*i.e.*, applicants' claimed invention). Office Action, page 14, lines 14-18.

This rejection, however, completely ignores important distinguishing features recited in claims 19 and 20. Claim 19 includes the following limitation related to the bracket and suspending the handset:

> the first major side of the handset having a straight portion or portions configured to contact a flat or generally flat surface when the handset is suspended by the bracket pressed against the flat or generally flat surface by a finger received in the finger-image sensor so as to stably maintain the handset during sensing of the finger.

Claim 20 includes the following limitation related to the bracket and suspending the handset:

> the first major sides of the first and second portions of the handset each having a straight portion which contacts a flat or generally flat surface when the handset is suspended by the bracket pressed against the flat or generally flat surface by a finger received in the finger-image sensor to maintain the handset steady during sensing of the finger.

In claim 19, structure of the handset is configured "so as to stably maintain the handset during sensing of the finger." In claim 20, the handset structure is "pressed against the flat or generally flat surface by a finger received in the finger-image sensor to maintain the handset steady during sensing of the finger."

This is not shown or suggested by Srey et al. as Srey et al. fails to even disclose a bracket. Official notice of a bracket for suspending a handset is not support for configuring a handset so that when suspended by a bracket, the handset is stably maintained against a flat surface or maintained steady during sensing of a finger. Without prior art disclosing or suggesting that a device such as a handset include a bracket and be configured so as to be maintained steady or stably during a finger image sense, the examiner is requested to allow claims 19 and 20.

IV. Drawing Objections Under 37 C.F.R. § 1.84(a)

Applicants submit herewith corrected formal drawings in compliance with 37 C.F.R. § 1.84(a).

V. Conclusion

The foregoing demonstrates that claims 1-9 and 11-20 are allowable. Thus, this application is in a condition for allowance. Reconsideration and allowance are therefore respectfully requested.

Respectfully submitted,

Frank J. DeRosa 1-6-03

Frank J. DeRosa, Reg. No. 26,543
Attorney for Applicants
Customer Number 29,858
Brown Raysman Millstein
Felder & Steiner LLP
900 Third Avenue
New York, NY 10022
Tel.: (212) 895-2003